Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (currently amended) An apparatus according to claim 58, further comprising:

a configuration storage in the isolated execution circuit to contain ~~containing~~ configuration parameters to configure ~~a~~ the processor in one of ~~a normal~~ the non-isolated execution mode ~~and an~~ or the isolated execution mode;

an access generator circuit coupled to the configuration storage to generate an isolated access signal ~~using~~ based on at least one of the configuration parameters and access information in a transaction, the isolated access signal being asserted when the processor is configured in the isolated execution mode; and

a bus cycle decoder coupled to the access generator circuit to generate an isolated bus cycle corresponding to a destination in the transaction, based on ~~using~~ the asserted isolated access signal and the access information.

A3

2-7. (canceled)

8. (currently amended) The apparatus of ~~claim 7~~ claim 1, wherein:

the configuration parameters comprise a memory setting to define an isolated memory area within memory external to the processor; and

the access generator circuit ~~comprises:~~ comprises an address detector to detect if ~~the physical address is within~~ physical addresses of transactions reference the isolated memory area ~~defined by the isolated setting~~.

9-15. (canceled)

16. (currently amended) A method according to claim 71, further comprising:

configuring ~~a~~ the processor in one of ~~a normal~~ the non-isolated execution mode ~~and an~~ or the isolated execution mode, based on configuration parameters in ~~using~~ a configuration storage in the processor~~, the configuration storage containing configuration parameters~~;

asserting an isolated access signal by an access generator circuit, based on ~~using~~ at least one of the configuration ~~isolated area~~ parameters and access information in a transaction when the processor is configured in the isolated execution mode; and

generating an isolated bus cycle corresponding to a destination in the transaction by a bus cycle decoder, based on ~~using~~ the asserted isolated access signal and the access information.

17-45. (canceled)

46. (new) A system comprising:

a processor that supports two or more operating modes with different levels of privilege, including a ring 0 operating mode and a higher ring operating mode;

a chipset communicatively coupled to the processor, wherein the chipset supports communication between the processor and a memory;

configuration storage within the processor to store configuration parameters comprising:

a first configuration setting to define an isolated memory area within the memory; and

a second configuration setting to switch the processor between an isolated execution mode within the ring 0 operating mode and a non-isolated execution mode within the ring 0 operating mode; and

an isolated execution circuit within the processor to generate isolated bus cycles when the processor executes in the isolated execution mode, wherein the isolated bus cycles enable a module to access a resource that is only accessible from the isolated execution mode of the ring 0 operating mode.

47. (new) The system of claim 46, wherein the isolated bus cycles generated by the isolated execution circuit comprise:

a data access cycle;

a control access cycle; and

a logical processor access cycle.

48. (new) The system of claim 46, wherein the isolated bus cycles generated by the isolated execution circuit comprise at least one isolated bus cycle selected from the group consisting of:

a data access cycle;

a control access cycle;

and a logical processor access cycle.

49. (new) The system of claim 48, wherein the isolated execution circuit generates the data access cycle in response to a transaction involving a reference to the isolated memory area.

50. (new) The system of claim 48, wherein the isolated execution circuit generates the control access cycle in response to a transaction involving an input/output reference to an isolated register in a chipset external to the processor.

51. (new) The system of claim 48, wherein the isolated execution circuit generates the logical processor access cycle in response to a transaction involving one of a logical processor entry to the isolated execution mode or a logical processor withdrawal from the isolated execution mode.

A4

52. (new) The system of claim 46, wherein the isolated bus cycles generated by the isolated execution circuit comprise an isolated bus cycle that enables access to at least one resource selected from the group consisting of:

the isolated memory area;

an isolated register; and

an isolated state.

53. (new) The system of claim 46, wherein the first configuration setting to define the isolated memory area comprises at least one value selected from the group consisting of:

a mask value;

a base value; and

a length value.

54. (new) The system of claim 46, wherein the first configuration setting to define the isolated memory area comprises a mask value, a base value, and a length value.

55. (new) The system of claim 46, further comprising:

a processor control register within the isolated execution circuit; and

an execution mode word in the processor control register that is asserted when the processor is configured in the isolated execution mode.

56. (new) The system of claim 46, further comprising:

a logical processor counter in the chipset that is updated in a first direction in response to a logical processor entry to the isolated execution mode and is updated in a second direction in response to a logical processor withdrawal from the isolated execution mode.

A4

57. (new) The system of claim 46, further comprising:

an access generator circuit in the isolated execution circuit and coupled to the configuration storage, the access generator circuit to generate an isolated access signal based on access information in a transaction and at least one of the configuration parameters, the isolated access signal being asserted when the processor is configured in the isolated execution mode, and

a bus cycle decoder in the isolated execution circuit and coupled to the access generator circuit, the bus cycle decoder to generate an isolated bus cycle corresponding to a destination in the transaction based on the access information and the asserted isolated access signal.

58. (new) An apparatus comprising:

a processor capable of supporting two or more operating modes with different levels of privilege, including a ring 0 operating mode and a higher ring operating mode, wherein the processor allows modules executing in ring 0 to access data associated with modules executing in the higher ring, but the processor does not allow modules executing in the higher ring to access data associated with modules executing in ring 0; and

an isolated execution circuit within the processor that supports bifurcation of the ring 0 operating mode into an isolated execution mode and a non-isolated execution mode, by allowing the processor to be switched between the isolated execution mode and the non-isolated execution mode, and by generating isolated bus cycles when the processor executes in the isolated execution mode.

A4

59. (new) The apparatus of claim 58, wherein the isolated bus cycles comprise:

a data access cycle;

a control access cycle; and

a logical processor access cycle.

60. (new) The apparatus of claim 58, wherein the isolated bus cycles comprise at least one isolated bus cycle selected from the group consisting of:

a data access cycle;

a control access cycle; and

a logical processor access cycle.

61. (new) The apparatus of claim 60, wherein the isolated execution circuit generates the data access cycle in response to a transaction involving a reference to an isolated memory area in a memory external to the processor.

62. (new) The apparatus of claim 60, wherein the isolated execution circuit generates the control access cycle in response to a transaction involving an input/output reference to an isolated register in a chipset external to the processor.

63. (new) The apparatus of claim 60, wherein the isolated execution circuit generates the logical processor access cycle in response to a transaction involving one of a logical processor entry to the isolated execution mode or a logical processor withdrawal from the isolated execution mode.

64. (new) The apparatus of claim 58, wherein the isolated bus cycles generated by the isolated execution circuit comprise an isolated bus cycle that enables access to at least one resource selected from the group consisting of:

an isolated memory area in a memory external to the processor;

an isolated register; and

an isolated state.

A4

65. (new) The apparatus of claim 64, wherein the isolated execution circuit generates at least one of the isolated bus cycles based on an access type and a destination of a transaction.

66. (new) The apparatus of claim 58, wherein the processor further comprises configuration storage to contain memory settings to define an isolated memory area in a memory external to the processor.

67. (new) The apparatus of claim 66, wherein the memory settings comprise at least one value selected from the group consisting of:

a mask value;

a base value; and

a length value.

68. (new) The apparatus of claim 66, wherein the isolated execution circuit comprises an address detector to detect if a physical address in a transaction is within the isolated memory area.

69. (new) The apparatus of claim 58, wherein the isolated execution circuit comprises a processor control register to contain an execution mode word that is asserted when the processor is configured in the isolated execution mode.

70. (new) The apparatus of claim 58, wherein the isolated execution circuit generates an isolated bus cycle based on an access type of a transaction.

71. (new) A method comprising:

receiving, at a processor, a first configuration setting to define an isolated memory area within memory external to the processor, wherein:

the processor supports two or more operating modes with different levels of privilege, including a ring 0 operating mode and a higher ring operating mode;

the processor allows modules that execute in ring 0 to access data associated with modules that execute in the higher ring; and

the processor prevents modules that execute in the higher ring from accessing data associated with modules that execute in ring 0;

receiving, at an isolated execution circuit of the processor, a second configuration setting to switch the processor between an isolated execution mode within the ring 0 operating mode and a non-isolated execution mode within the ring 0 operating mode; and

generating isolated bus cycles with the processor executing in the isolated execution mode, wherein the isolated bus cycles enable a module to access a resource that is only accessible from the isolated execution mode of the ring 0 operating mode.

72. (new) The method of claim 71, further comprising:

initializing the isolated execution mode, using a processor nub loader;

loading a processor nub into the isolated memory area, using isolated bus cycles; and

verifying an operating system nub, using the processor nub.

73. (new) The method of claim 72, further comprising:

if the operating system nub verifies as good, loading the operating system nub into the isolated memory area, using isolated bus cycles.

74. (new) The method of claim 71, further comprising:

loading a processor nub into the isolated memory area, using isolated bus cycles;

loading an operating system nub into the isolated memory area, using isolated bus cycles; and

generating platform verification data, based on attributes comprising:

a platform key;

the processor nub; and

the operating system nub.

75. (new) The method of claim 74, further comprising:

A4

switching from the isolated execution mode to the non-isolated execution mode; and

loading an operating system kernel into non-isolated memory.

76. (new) The method of claim 75, further comprising:

switching from the ring 0 operating mode to the higher ring operating mode; and

executing an application in the higher ring operating mode.

77. (new) The method of claim 71, wherein the operation of generating isolated bus cycles comprises generating at least one isolated bus cycle selected from the group consisting of:

a data access cycle;

a control access cycle; and

a logical processor access cycle.

78. (new) The method of claim 77, wherein the operation of generating at least one isolated bus cycle comprises:

generating the data access cycle in response to a transaction involving a reference to the isolated memory area.

79. (new) The method of claim 77, wherein the operation of generating at least one isolated bus cycle comprises:

generating the control access cycle in response to a transaction involving an input/output reference to an isolated register in a chipset external to the processor.

80. (new) The method of claim 77, wherein the operation of generating at least one isolated bus cycle comprises:

generating the logical processor access cycle in response to a transaction involving one of a logical processor entry to the isolated execution mode or a logical processor withdrawal from the isolated execution mode.

A4

81. (new) The method of claim 71, wherein the operation of generating isolated bus cycles comprises generating an isolated bus cycle that enables access to at least one resource selected from the group consisting of:

the isolated memory area;

an isolated register; and

an isolated state.

82. (new) The method of claim 71, wherein the operation of receiving a first configuration setting to define an isolated memory area comprises receiving at least one value selected from the group consisting of:

a mask value;

a base value; and

a length value.

83. (new) The method of claim 71, further comprising:

asserting an execution mode word in a processor control register within the isolated execution circuit when the processor is configured in the isolated execution mode.

84. (new) The method of claim 71, further comprising:

in response to a logical processor entry to the isolated execution mode, updating a logical processor counter in a chipset in a first direction.

A4

85. (new) The method of claim 84, further comprising:

in response to a logical processor withdrawal from the isolated execution mode, updating the logical processor counter in the chipset in a second direction.